Защита от нежелательной отспамов в Exchange Server

ПРИМЕНЯЕТСЯ К: ✅ 2016 ✅ 2019 ✅ по подписке

Спаммеры или вредоносные отправители используют различные методы для отправки нежелательной электронной почты в вашу организацию. Не существует единого средства или процесса, с помощью которого можно устранить весь спам. Тем не менее в Microsoft Exchange реализован многоуровневый и многогранный подход к сокращению количества таких сообщений. Exchange использует агенты транспорта для защиты от нежелательной информации, а встроенные агенты, доступные в Exchange Server 2016 и Exchange Server 2019 годах, относительно не изменились по сравнению с Exchange Server 2010 г. В Exchange 2016 и Exchange 2019 настройка этих агентов и управление ими доступны только в командной консоли Exchange.

Для более простых функций защиты от нежелательной почты и упрощения управления приобретите встроенную надстройку безопасности для локальных почтовых ящиков. Дополнительные сведения о защите от нежелательной почты в облаке см. в статье Защита от нежелательной почты для облачных почтовых ящиков.

Агенты защиты от нежелательной почты на серверах почтовых ящиков

Как правило, агенты защиты от нежелательной почты включаются на серверах почтовых ящиков, если в организации нет пограничного транспортного сервера или не выполняется дополнительная фильтрация входящих сообщений. Дополнительные сведения см. в разделе Включение функций защиты от нежелательной почты на серверах почтовых ящиков.

Как и всем агентам транспорта, каждому агенту защиты от нежелательной почты назначается значение приоритета. Чем ниже значение, тем выше приоритет, поэтому агент с приоритетом 1 обычно применяется к сообщению раньше агента с приоритетом 9. Тем не менее событие SMTP транспортного конвейера, в котором зарегистрирован агент, также очень важно для определения порядка, в котором агент защиты от нежелательной почты обрабатывает сообщения. Агент с низким приоритетом, зарегистрированный на более раннем этапе транспортного конвейера, выполняется перед агентом с высоким приоритетом, который был зарегистрирован в транспортном конвейере позже.

С учетом значения приоритета агента по умолчанию и события SMTP, в котором он зарегистрирован, агенты защиты от нежелательной почты применяются к сообщениям на серверах почтовых ящиков в следующем порядке:

1. **Агент фильтрации отправителей**. Фильтрация отправителей сравнивает отправляющий сервер со списком отправителей или доменов отправителей, которым запрещено отправлять сообщения в организацию. Дополнительные сведения см. в разделе Фильтрация отправителей.
2. **Агент идентификатора отправителя**. Идентификатор отправителя зависит от IP-адреса отправляющего сервера и предполагаемого ответственного адреса (PRA) отправителя, чтобы определить, является ли адрес электронной почты отправки поддельным. Дополнительные сведения см. в разделе Sender ID.
3. **Агент фильтра содержимого**. Агент фильтрации содержимого назначает каждому сообщению уровень достоверности нежелательной почты (SCL) на основе данных из допустимых и нежелательных сообщений. Дополнительные сведения см. в разделе Фильтрация содержимого.

   Карантин спама — это компонент агента фильтра содержимого, снижающий риск потери подлинных сообщений, ошибочно определенных как спам. Он представляет собой временное место хранения для подозрительных сообщений, где их может проверить администратор. Дополнительные сведения см. в разделе Карантин спама в Exchange Server.

   При фильтрации содержимого также используется функция объединения списков надежных отправителей. Объединение списков надежных отправителей собирает данные списков надежных отправителей, которые пользователи настраивают в Microsoft, Outlook и Outlook в Интернете, и делает эту сведений доступных для агента фильтра содержимого. Дополнительные сведения см. в разделе Объединение списков надежных отправителей.

4. **Агент анализа протоколов (репутация отправителя):** агент анализа протоколов — это агент, обеспечивающий репутацию отправителя. Он выполняет ряд проверок, чтобы вычислить уровень репутации отправителя (SRL) для входящих сообщений, по которому затем определяется действие, выполняемое с этими сообщениями. Дополнительные сведения см. в разделе Sender reputation and the Protocol Analysis agent.

Агенты защиты от нежелательной почты на пограничных транспортных серверах

Если в сети периметра организации установлен пограничный транспортный сервер, на нем устанавливаются и по умолчанию включаются все агенты защиты от

нежелательной почты, доступные серверу почтовых ящиков. Однако следующие агенты доступны только на пограничных транспортных серверах:

- **Агент фильтрации подключений**. Фильтрация подключений использует список заблокированных IP-адресов, список разрешенных IP-адресов, поставщики списков блокировок IP-адресов и поставщики списка разрешенных IP-адресов для определения того, должно ли быть заблокировано или разрешено подключение. Дополнительные сведения см. в разделе Фильтрация подключений на пограничных транспортных серверах.
- **Агент фильтра получателей**. Фильтрация получателей использует список блокировок получателей для идентификации сообщений, которым запрещено входить в организацию. Фильтр получателей также использует локальный каталог получателей для отклонения сообщений, отправленных недопустимым получателям. Дополнительные сведения см. в разделе Фильтрация получателей на пограничных транспортных серверах.

  Примечание.

  Хотя агент фильтра получателей доступен на серверах почтовых ящиков, его не следует настраивать. Если при фильтрации получателей на сервере почтовых ящиков в сообщении обнаруживается по крайней мере один недопустимый или заблокированный получатель, сообщение отклоняется. Агент фильтра получателей активируется, когда вы устанавливаете агенты защиты от спама на сервере почтовых ящиков, но не блокирует получателей.

- **Агент фильтрации вложений**. Фильтрация вложений блокирует сообщения или вложения на основе имени файла вложения, расширения или типа контента MIME. Дополнительные сведения см. в разделе Фильтрация вложений на пограничных транспортных серверах.

С учетом заданного по умолчанию значения приоритета агента и события SMTP транспортного конвейера, в котором зарегистрирован этот агент, агенты защиты от нежелательной почты применяются к сообщениям на пограничном транспортном сервере в следующем порядке:

1. Агент фильтрации подключений
2. Агент фильтра отправителей
3. Агент фильтра получателей
4. Агент идентификации отправителей
5. Агент фильтра содержимого
6. Агент анализа протокола (репутация отправителя)
7. Агент фильтрации вложений

Метки нежелательной почты

Метки нежелательной почты применяются к сообщениям и используются агентами защиты от нежелательной почты. Вы можете просматривать метки нежелательной почты, чтобы выявлять проблемы, связанные со спамом. Дополнительные сведения см. в разделе Метки защиты от нежелательной почты.

Стратегия защиты от нежелательной почты

Защита от нежелательной почты — это баланс между блокированием нежелательных сообщений и разрешением подлинных. Если настроить слишком много функций строгой защиты от нежелательной почты, высока вероятность блокировки множества подлинных сообщений (ложных срабатываний). Если же сделать защиту слишком свободной, в организацию будет проникать много спама.

Ниже приводятся некоторые рекомендации, которые следует учитывать при настройке встроенных функций защиты от нежелательной почты в Exchange.

- Отклоняйте сообщения, определяемые агентом фильтрации подключений, агентом фильтра получателей и агентом фильтра отправителей, а не карантином сообщений или применением меток защиты от спама. Этот подход рекомендуется по следующим причинам:
    - Как правило, сообщения, обнаруженные при использовании параметров по умолчанию для фильтрации подключений, получателей и отправителей, можно считать нежелательными без дальнейших проверок. Например, если для фильтрации отправителей настроена блокировка определенных отправителей, нет необходимости продолжать обработку сообщений от этих отправителей. (Если вы не хотите, чтобы сообщения отклонялись, вы бы не поместили их в список заблокированных отправителей).
    - Настройка более агрессивного уровня для агентов защиты от спама, которые сталкиваются с сообщениями на ранних этапах транспортного конвейера, позволяет сэкономить ресурсы обработки, пропускной способности и дисков. Чем дальше сообщение проходит по транспортному конвейеру, тем больше переменных приходится учитывать оставшимся компонентам защиты от нежелательной почты, чтобы успешно определить сообщение как спам. Отклоняйте очевидный спам как можно раньше, чтобы оставить время для подозрительных сообщений.
- Необходимо отслеживать эффективность функций защиты от нежелательной почты на их текущих уровнях конфигурации. Мониторинг позволяет реагировать на тенденции, а также повышать и понижать интенсивность защиты. Для начала следует использовать параметры по умолчанию, чтобы свести к минимуму число ложных срабатываний. По мере отслеживания

количества спама и ложных срабатываний вы можете повышать интенсивность защиты в зависимости от типов спама и атак, наблюдаемых в организации.